
# Atlantic Council Community Watch: China's Vision for the Future of the Internet

## December 4 2023

**Colleen Cottle:** Hello everyone, and thanks for joining us for today's event, Community Watch, China's Vision for the Future of the Internet. My name is Colleen Cottle, Deputy Director of the Atlantic Council's Global China Hub, which devises allied solutions to the global challenges posed by China's rise.

In doing so, it leverages the Atlantic Council's work on China across its 16 programs and centers. In 2015, China released a white paper called Jointly Building a Community with a Shared Vision in Cyberspace. It was aimed at rallying the international community around China's vision for global cyberspace news.

Its particular focus on cyber sovereignty appealed to non-democratic and illiberal developing nations. According to this concept, individual states should have the right to determine the content, operations, and norms of Internet usage within their borders. In addition, the concept asserts that all states should have equal say in the administration of the global Internet.

Today, the production of the concept of a shared future for the Internet remains front and center in China's strategy for engagement with its allies. Every year, China convenes international organizations Global Internet Enterprises and Industry Associations and Research Institutes from around the world for the World Internet Conference in Wujian.

This year's event, the 10th anniversary of the conference, was themed Creating an Inclusive and Resilient Digital World Beneficial to All. In his opening address, Xi Jinping called for a more equal and inclusive space. and the expansion of Internet

infrastructure in the Global South. China couches its approach in lofty terms as advancing a shared future of humanity.

However, in practice, it makes the world safer for authoritarian governments. Internet connectivity is vital for economic development, but with greater connectivity comes improved communication among dissidents. Beijing understands this problem, and it's trying to advance global norms that facilitate the provision of its censorship and surveillance tools to other countries, as a way to offer political security to illiberal governments.

Reducing the risk of political stability also makes the operating environment safer for Chinese firms active in these countries. In addition to its implications for freedom, democracy, and human rights, there is also an important security dimension to this concept of a community with a shared future in cyberspace.

This is particularly true when it comes to operations of state backed hacking teams. Chinese cybersecurity firms are expanding their customer base globally. As they do so, these firms gain access to a more complete view of cyber incidents, which they are required to report to Beijing. This, in turn, increases the Chinese government's visibility into the global cyber operations of other nations or of transnational criminal groups.

It also aids China's offensive hacking efforts. They'll need to do less of a lift as China security services are likely to operate, unimpeded in cybersecurity firm's customer networks. With these complex dynamics at play, we are happy to host today's launch of a new report by Global China Hub, non-resident fellow Dakota Carey.

In this paper, Dakota walks us through the principles behind the community with the shared future in cyberspace. and China's motivations for operationalizing this vision. It also examines two case studies of countries receptive to China's approach. The Solomon Islands and Russia. The report is available on the Global China Hub's website now, and we've gathered a fantastic group of experts to discuss the issues he delves into.

Before we kick off our panel, it's my pleasure to introduce our moderator, Jamie Tarabay. Ms. Tarabay is a reporter for Bloomberg based in Washington, D. C., who has also covered cybersecurity issues across the Asia Pacific region. She has been involved in the global coverage of cyber espionage and sabotage and cyber attacks, including SolarWinds, the JBS and Colonial Pipeline hacks and others.

She joined Bloomberg in 2020. She has been a reporter and editor for more than 20 years, covering conflicts in the Middle East and Southeast Asia, as well as environmental disasters, racial violence, and elections in the US, Europe, and Australia. She has been recognized with awards. for her coverage of the Iraq war and protests in Ferguson.

She was previously a correspondent for the New York Times. Ms. Tarabay, we're happy to have you join this discussion. Over to you.

**Jamie Tarabay:** Good morning and thank you so much for having me. I'm so happy to be here today to introduce Dakota Carey and his report. I've read it already and I'm really excited about the conversation that we're going to be having once he's finished walking you all through it.

Dakota Carey is a non-resident fellow at the Atlantic Council's Global China hub, he's also a consultant at Krebs Stamos Group. Before that, he was a research analyst at Georgetown University Center for Security and Emerging Technology on the Cyber AI project. His focus has been on China's efforts to develop attacking capabilities, artificial intelligence, and cybersecurity research at Chinese universities, the people liberate the People's Liberation Army's efforts to automate.

Software vulnerability discovery and new policies to improve China's cybersecurity talent pipeline. His work has appeared in the Economist, the MIT Tech Review, the Hill Breaking Defense and Defense Fund. Dakota has also testified before the US China Economic and Security Review Commission. I'm going to leave it to him now to walk us all through the report and then we'll join in with a conversation with our experts.

When he's done.

**Dakota Cary:** Hey there, thanks so much for joining. I'm really happy to talk through today's issue. I figured I'd start us, about a decade ago in 2014 in Wujing, China, at the first, World Internet Conference. Attendees had sat through three days of conference talks on how 5G was going to be the future of the internet and interconnectivity is going to change everything, et cetera.

And on the last evening of the conference, folks who had organized it ham fistedly shoved papers under conference attendees doors around 11 p. m. and were like, hey, tomorrow morning, can you sign this document? A lot of people have asked for it, and we think it represents the views of all the attendees.

The folks who attended, which included, a bunch of representatives from, foreign governments, as well as the private sector, were shocked at this approach, to trying to get a diplomatic document signed, and so it went unsigned, and, in, in 2015, the Chinese government decided that in order to get folks on board with this vision that they wanted to lay out for the future of the Internet, its regulations on contents, norms and operations, was that they needed Xi Jinping to headline it.

And so in 2015, he headlines the conference, and he makes clear, what he's aiming for the future of the internet to look like. The basic deal for, the PRC and, nations abroad is effectively to say that if you're an illiberal democracy, if you are a developing nation, if

you're an authoritarian government, and you're concerned by internet connectivity, but you want the benefits of digitizing trade, e commerce, social networks and collaboration, digitizing your monetary system.

We can help you build the infrastructure for that in a way that does not risk your political system. China, like other authoritarian governments, had watched the Arab Spring. With horror, at what, interconnectivity between political dissidents had allowed and facilitated, and so its vision for the future of Internet, regulation, Internet norms was centered around addressing interconnectivity in a politically safe way for authoritarian governments.

So, in 2015, Xi outlines his proposal, with four principles. The first being, the respect for cyber sovereignty. This principle kind of drives everything else. the PRC attaches cyber sovereignty directly to the UN Chartered Nations, so it is stating that, very clearly, because we are a state, we have these natural rights imbued to us, and that includes deciding what is and is not appropriate on the Internet within our borders, how the Internet is structured, who is able to access it, etc.

And then he has three subsidiary, or like, follow on principles. that kind of describe the implementation of, this shared vision. Those are maintenance of peace and security, the promotion of openness and cooperation, and the cultivation of good order online. Each of these three things are more closely tied to specific, policy objectives, maintaining peace and security.

And in the report, we put Xi Jinping's direct language in there, but he effectively says that, hacking against government targets and the theft of commercial IP are equivalent, in Western capitalist nations, we hold these, in different light, commercial IP theft. Is not something that we would consider to be equivalent to hacking into a foreign government in order to collect political or military intelligence.

So there is, a pretty significant disconnect between how we interpret what is or is not, acceptable in cyberspace. And then that principle really underlines this promotion of, openness and cooperation, as well as cultivating good order, both of which are, effectively laying the ground for content censorship, surveillance, etc.

In furtherance of promoting what China views as good order online. And we'll get into examples of what that looks like. There is a report from the Communication University of China, in partnership with the Institute for Community with the Shared Future. Their report is called the report on online violence, and it details a number of case studies and what would count as online violence.

It would contravene the four principles set out in, creating a shared future, in cyberspace. That report details the, discussion, online discussion of COVID 19 starting in Wuhan, China. As an example of online violence, or the discussion of a deadly bus crash

in which a couple dozen people died in China, a discussion of that news as online violence.

And so the report itself makes quite clear that the discussion of things that are not appropriate, not politically palpable to Beijing would count as Online violence. It's a good example of what China is trying to push for at the UN. So in January of 2023, China pushed to make the dissemination of disinformation and international crime at the UN.

The resolution, or excuse me, their proposal was not adopted. However, it see what China's goals are for the international community within kind of a broader context to say if you're disseminating information that is against the interests of the Chinese Communist Party, we would like the ability to criticize your government for allowing you to do so, even if you're in your own country.

We've seen good examples of how, this has played out within China, just, the broader surveillance and censorship system applied domestically, rolling out abroad. However, there are two kind of good examples of what happens at either end of governments who are attempting to adopt this framework or structure.

The first being the Solomon Islands with, relatively immature capabilities for censorship and surveillance, domestically. In 2022, the Solomon Islands had a document link that showed, the government was considering hosting a PLA Navy base, for China's military. The US, Australia, New Zealand, freaked out.

We sent diplomats over and we said, please don't sign this document. The Solomon Islands government prevaricated. They said, we're not going to sign. It's not even real, et cetera. And for about two months, everything was fine. And then the Solomon Islands delayed elections for the prime minister.

in that process, he sent his personal security guards to China for additional training. He moved forward with signing the agreement for the Navy base. And then the China Export Import Bank facilitated the purchase of Huawei telecommunications kit. Effectively giving the PRC the ability to provide, political surveillance, within the Solomon Islands.

And the deal being, if you permit this naval base to go through, we will help keep you in power, for the duration, that you wish. At the other end of the spectrum, countries with more mature, preexisting abilities to conduct surveillance and censorship would be Russia.

And the late 20 teens, Russia and China actually signed an agreement at the Wujing Internet Conference that would help facilitate the transfer of expertise between these two systems. Russia was particularly interested in China's ability to conduct online censorship, as well as prevent people from using VPNs.

China was interested in learning from Russia about the promotion of, a positive state's image, et cetera, online. And so we do see, other countries trying to operationalize, these values. And then finally, on this point, I think that What's most interesting is when countries sign up for and try to institute, this type of vision for internet censorship and surveillance.

Chinese goods, in internet and communications infrastructure are particularly good at facilitating censorship and surveillance because they've honed those skills at home. And so the purchase of them abroad makes that transfer easier. Obviously, there are humans that have to be involved, technicians that facilitate this type of work.

However, we have seen instances where this is occurring. and then as we noted at the top, I think that the ability for this infrastructure to be used to facilitate China's meddling in other countries domestic politics is particularly important. A lot of, middling countries who are in the process of developing are doing so by extracting resources that are in their countries, et cetera.

And China tends to be an end consumer of many of those goods. China does not have the ability to compel, many governments to keep their word on contracts. Its military is not really capable, of transiting, all the way to another country and then threatening enough, to effectively compel another nation to abide by, something that it sees not in its favor anymore.

But when China is able to tie political surveillance and kind of political protection for the person in charge, as in the Solomon Islands, it becomes easier or as a point of leverage over that government, try to maintain or compel their actions on a particular policy area. And so while this paper tends to focus on content, surveillance and censorship, it does also have implications for the way that China interacts with other countries, and at this point I'd turn it back to Jamie and we can open it up to the panel.

**Jamie Tarabay:** Thank you. This is, we've got so much to talk about. We will also have the opportunity for questions, after a little chat with the panelists. Let me introduce the two other folks who are going to be joining us.

Tom Hegel is the principal threat researcher with Sentinel Labs at Sentinel 1. He's a cybersecurity researcher with a history of tracking some of the most unique threat actors globally. He's uncovered and published numerous discoveries of state sponsored actors across Russia, China, Iran, North Korea, India, and more, as well as new mercenary groups, and financially motivated crime work gangs. Tom is a dedicated advocate of humanitarian cyber security research initiatives, focusing on fortifying security measures and gathering intelligence on attackers who target high risk individuals and organizations.

Mallory Nodal is the Chief Technology Officer at the Centre for Democracy and Technology. She's a member, this is a mouthful, member of the Internet Architecture

Board and the Co Chair of the Human Rights Protocol Considerations Research Group of the Internet Research Taskforce. Mallory is also on the advisory committee for the Open Technology Fund. She takes a human rights, people centered approach to technology implementation with a focus on encryption, censorship, and cyber security.

So, welcome everyone. Dakota, thank you. This has been so much work. I do want to start with you and then we can ask everyone else to chime in. The report combines ideas of surveillance and censorship with traditional hacking. And usually these two ideas are considered separately. Can you expand a little on why they're overlapping in this report?

**Dakota Cary:** Yeah, absolutely. So, I think that they're typically held separate just by way of, how folks in the United States or in Western countries tend to think about these two issues. However, the offensive hacking that governments do for keeping track of political dissidents, or, furtherance of some other means are occurring on, It's happening on somebody's hardware.

It's happening on somebody's network. And the overlap between these two, is pretty evident from the operational standpoint. There's evidence of, work in Uganda by Huawei technicians to facilitate surveillance of political dissidents. There's instances at the Africa Union where data that was being stored on Chinese made kit was being transferred back to the PRC, at regular intervals. Although these two ideas are talked about separately, they have different policy mechanisms, the ability and the control over internet infrastructure can facilitate and oftentimes does facilitate, hacking operations, which we would, bucket under cybersecurity, generally is a different topic.

**Jamie Tarabay:** Mallory, in terms of China's vision regarding the Internet, how does that play out with international standards bodies?

**Mallory Knodel:** Yeah, so, China's very involved in global standards setting for the Internet. We see their presence all over from the hardware layer at the IEEE, so this is the International Institute for Electronics and Electrical Engineers, all the mouthfuls, I have all the acronyms I have to remember.

So they're working, obviously, at the hardware layer, they're working at the network layer, they're, Huawei is a huge implementer of 5G. It's working to devise the 6G standard in the International Telecommunication Union. And then they're also very present where I work, at the Internet Engineering Task Force.

This is where the Internet protocols are really decided upon. You see them at all layers. You see them very active, disproportionately so, based on their population. Like you do tend to see diversity in ITU because all UN member states are there.

But then, in the sort of open multi stakeholder or even industry standards bodies, you see actually China has almost an outsized presence. They are chairing a lot of groups. They are attending in large numbers. They're sending their best and brightest. And we've seen this also allows them to forum shop their ideas. The future of the internet that they've devised is almost a redesign of what we consider to be the Internet's protocol stack.

I don't have a chart for you. You don't want to see me, give you a slide deck on how the Internet works. But basically, they're questioning, why are we still using this outdated protocol stack, maybe we could achieve more efficiency if we redesigned it from the beginning. Of course, their redesign includes a lot of data rich signals that the network would have more information on who's sending the data and receiving the data, more information on what's being accessed, and that sort of thing.

So, it would facilitate much more fine grained privacy violations, surveillance, and censorship. And so it's ultimately an information control project throughout the entire stack from hardware chips, all the way up to application layer. And so, once they introduce these ideas, a lot of engineering communities are not in favor of them because they do have these risks, they do pose these problems, and so they'll take the idea from forum to forum until they find a place where the group would be more amenable.

The ITU, for example, is a place where there's a lot more interest in these ideas than there would be in an industry led or an open multi stakeholder forum like the IETF.

This forum shopping doesn't always work. So far for what China calls new IP, this redesign of the internet protocol stack, it hasn't taken off, but we do see them changing their arguments.

Now they've moved away from these efficiency arguments, because I think the pandemic showed that, though Internet as it's designed is actually quite rather resilient and robust, they've now discussed green IP, so this idea that you could get more environmental sustainability benefits from redesigning the whole protocol stack.

I note also what Dakota's saying is, well, we're hearing a lot of, now, sort of process point criticisms of these open multi stakeholder forums, because they're not diverse enough. They don't include global self voices. The ITU does. The ITU is amenable to these ideas. The ITU has all the member states there.

They're able to compel more sort of sympathy, and more ideas, from countries in the global south because they also then offer blueprints from, not just here's the protocol stack, but here's how you could implement it along with these other products and, sort of part of their Belt and Road initiative as well.

So, I would just leave you with saying that this is all really a project of more and increased information controls so that the entire Internet stack is essentially complicit in these activities, and there's no way to get around them or circumvent this.

**Jamie Tarabay:** That's so interesting. I have so many questions.

We have a late addition to our panel, Emily de La Bruyère, who's a senior fellow for the Foundation for Defense of Democracies. Thank you so much for joining us, Emily. I don't know if you were able to get a handle on, Dakota's report, but if there's something that you'd like to mention now, it would be great to have you, to

hear from you.

**Emily de La Bruyère:** I mean, I think, and a lot of this was already just said in the answer, and also apologies for joining late, but there's like a fundamental assumption underlying the excellent work, and I think it's important to tease out, which is also very clear in the report, which is just the degree to which China is able to combine a number of different strategic or competitive, or influence oriented types of international engagement, and in a way that risks being asymmetric to how the rest of the global order, whether that's international organizations like the ITU or other nation states are organized, and therefore stymieing their efforts or tools to respond.

That's seen in the overlap of industrial or technical power and norms, or security type influence that Beijing's able to manipulate in its digital and internet ambitions, and that's in a world where those types of influence or types of power tend to be separated. There's no really good answer to that.

Organizations that are focused on technical cooperation tend not to be oriented towards strategic or ideological power and leverage and development, and vice versa. That's creating a real handicap or hurdle for the global order, even as it recognizes, to some extent, the nature of what Beijing's trying to do and the strategic implications.

Even just having that approach, which is evident in this report, is really pretty groundbreaking in terms of how we think about what China's doing and how we need to respond.

**Jamie Tarabay:** Thank you.

Tom, I wanted to talk to you because the Solomon Islands example is such a clear one for us. I mean, I was based in the Asia Pacific for many years and I remember when this leaked memo came out and then of course, you sort of watch the back and forth that went through until, as Dakota mentioned, the mobile cell tower contract came through.

I remember KPMG did an audit of the contract and they basically concluded that there was no way that there would be ever enough revenue that could pay for the contract, by the time the towers came online, they would already be redundant and the tech would be too old. We talk about this a lot.

We had the data center in Papua New Guinea, and there's obviously a specific focus on the Pacific Islands per se. Can you sort of contextualize that for us in terms of sort of the global reach, particularly when it comes to sort of China's cyber security operations, and how it looks on the ground when it is in hand with a territorial sort of sovereignty question as well?

**Tom Hegel:** Yeah, absolutely. It's a fascinating topic, and there's so many particular points about China's offensive actions that really do such well highlighting of the diversity and importance they play on different sectors. Obviously, this conversation is really heavily leaning toward the telecommunications and so forth, leaning into the Solomon Islands, anything we see in Africa, it does tend to have, a very standard nature of political espionage or just intelligence collection for pre positioning for conflict in the future for China.

They're looking to, in many cases, get their hands in and have their technology relied on in parts of the world that might not be critical yet, but that they see as critical on the global scale within the coming decades. Solomon Islands is a fantastic example because it's just like so clear, and all the way leading up to the hacking by specific Chinese attributed threat actors that we track, to do information collection. That's just really one example of just them diving in, and trying to understand the scenario using offensive actions, through their hacking collectives.

There's quite a few examples throughout North Africa that we've been tracking over the last year or so that. Focus on telecommunications as well, rather than just, information about is this base going to happen or not? Communication infrastructure is really important. We see them targeting competing organizations in Africa that would be competing against Huawei deployments and so forth.

Ultimately the summary of it is, over the last decade or so, we've seen Chinese threat actors lean really heavily into intellectual property theft, trying to build their capabilities, become a reliant technology sources. And today, it's almost like we're seeing them push to deploy that, make them the number one source for technology, specifically in the global south, and then it'll transfer to greater scale.

But, yeah, so it's a little bit of everything in terms of where they're targeting, but communication is important. One thing that I think is really critical is the digital financial networks as well. Africa, going through their heavy reliance on like mobile money platforms, that's now being taken over by Chinese organizations as well. So you think of almost an entire continent that's reliant on China's mobile processing capabilities for them to operate domestically and on a world scale. That's a huge reliance on China. And

that's certainly a capability China would pursue for, being able to sway them politically or strategically throughout the coming years.

**Jamie Tarabay:** So, Dakota, I wanted to ask, because we've talked about this a little and this idea of there going to be two Internets or at least, there's a clear philosophical, geopolitical, division here between countries that have banned Huawei and countries that are embracing Huawei, and what that actually means for... ,

What can you tell us about the countries that are supportive of China's shared future policy? And, I mean, is there a list or something that we could access?

**Dakota Cary:** Absolutely. I'm interested to hear what Mallory's got to say about the idea of multiple Internets, and so I'll kick it to her when I wrap up on the political stuff.

Who is participating is not readily available, even in the paper that is accompanying, Xi Jinping's 2015 speech. There's a white paper that's gone out with it, most recently re-released in 2022. The list of countries who are supporting this idea, is not public.

I reached out to an organization to determine, like, it says that they work with 33 national CIRTs, which are, critical incident response teams. So, it's either like national bodies that tend to dispatch incident responders when something bad happens to government infrastructure, et cetera.

China states that it works with, 30 plus other governments on this, but when I asked for that data, they didn't provide it. There are many instances of which, where a bilateral agreement has been announced and is covered in press, and that is probably the best heuristic for who is participating in this kind of like pushing for this style of norms or governance.

The Solomon Islands having signed an agreement in mid 2023 on cybersecurity with China. Cuba is among those, Russia. But there are a number of countries that are frequently mentioned either in the report or in academic or other institutions that are working on this topic. Pakistan has a university with its own center for a community with a shared future. However, besides just cyberspace, it also includes, other centers, besides just that one, and there are a number of Middle Eastern and North African countries that are pretty consistently listed as people that China is participating with, but, perhaps, they don't go as far as to say these people have signed on to some formal document, that embodies our values.?

**Jamie Tarabay:** Mallory?

**Mallory Knodel:** Yeah, happy to jump in on this question of internet fragmentation because we do hear this a lot as the threat is, our internet's going to start breaking into pieces. I will start with the good news, or a more sunny approach to this, which is that

what I was saying before about China's presence in these global standards bodies is an indicator that we're not that far gone yet.

And, it's really important to foster that global cooperation and to not, for example, think about overstepping or banning or things like that. We had a moment, right when Huawei and Chinese companies were banned in the U. S. with a Bureau of Commerce rule, and the IEEE overnight had to de-chair a bunch of folks from Huawei. That was corrected a few days later, with an exemption to that rule, but it was a panic situation because we actually really do need that cooperation. And I would take it a step further on the solution side, which is that we also need more reasons and continue to hold on to the existing reasons we have to have a global interoperable Internet.

Tom mentioned financial institutions. That is a core reason why we will continue to see one Internet and the one that we have now, rather than some new thing that might, operate in parallel. The fewer reasons we have to have this sort of global interoperable internet, the less likely we are to keep it.

We will then see a proliferation of different kinds of internet that don't always work in, the same way across the globe. I would say that I would have to take it a step further. So that's when we have, global integration, across the most necessary, sort of global functioning, processes, but then people and individuals will continue to suffer unless we really think about how to strengthen the existing internet and create opportunities for circumvention of these kinds of fragmentation. And that is something that I think. While the private sector in the sort of more open democratic countries have really focused on privacy.

That's been great. It's been an anti surveillance tool. You get some circumvention effects with privacy enhancing technologies and with, privacy by design, but circumvention is a whole different set of, gives you a whole different set of benefits, and I think we need concerted effort by those same companies, hopefully more companies as well, especially when we're talking about cybersecurity, to really focus on this element of circumvention.

Otherwise, end users in all of these countries, whether it's Uganda or China itself, Iran, et cetera, will not see this sort of unfragmented Internet. They will continue to see it at the user level as rather fragmented, and so I feel like that's maybe a big risk. That we see before us. So I'll leave it at that.

**Jamie Tarabay:** Thank you. I wanted to actually go to Tom about this. In terms of what are the insights that you've been able to glean from, so Chinese state sponsored offensive cyber activity, particularly in places like for the global south, for example, and, what is the connection, with the working group in the report and, and also just, like the sort of follow on from that is how.

And this, clearly impacts, some of the African networks that we've just discussed, how might PRC manufactured technical infrastructure in these countries impact the defensive capabilities or the position of that country?

**Tom Hegel:** Yeah, great question. So, I think the most simple example, within like the, African nation context is seeing the African Union, their intrusions that kind of steps into both scenarios.

So, in that case, what we have just a quick catch up is. The African Union, new headquarters was operating after being built and funded by Chinese investments, operating for, I believe, about five years. And, in 2017, IT staff identified the intrusion into their network. That was actually not necessarily intrusion, but their equipment was actually exfiltrating information back to China, specifically video, surveillance footage and, and so forth, so remote access capabilities, and reportedly that was all Huawei technology.

From like a technical perspective, we view that as you don't need to put a backdoor in the network when it already exists through the equipment, to be blunt. After the remediation of that, a couple of years later, we see third party vendors like myself that are identifying intrusions into the African Union networks that are attributed to cyber threat actors, back to state sponsored Chinese entities, specifically like APT 17 and so forth. The offensive hacking kind of shows a priority of this organization to Chinese intelligence collection needs. We see that actor actually seeking out surveillance footage, through archaic, replaced Huawei equipment in the network.

So, that kind of shows you an example of the priority they place on leading political organizations within Africa. We see that same type of stuff all throughout Africa by a variety of different, threat actors attributed to China.

Like I mentioned, telecommunications is such a huge one. We see them going after competing telecommunication organizations, spreading throughout Africa. Anything that would put a threat to Huawei's dominance in Africa is considered a ripe target. And then financial organizations, as you step really closely into that debt trap diplomacy, similar to Solomon Islands, they want to do information collection on organizations that they want to know if the finances are stable, because China is doing such a heavy amount of investment throughout Africa.

So it puts a weird strain on African organizations that are clearly being hacked by Chinese state sponsored actors, but then on the other side are being funded and supported and given resources by Chinese investments. So they're in a position where they don't want to publicly call out China for their hacking operations. You see a lot of silence and we have to lean really heavily into the technical realm to identify much of this.

But that's really where our working group steps up that, Dakota mentioned in his report, started noticing big gaps in intelligence collection from the specifically Western cybersecurity organizations. We're pretty blind to what's actually happening throughout Africa, Latin America included in that as well. The global South is just a blind spot for us. So we started a working group to try and collectively understand what's happening within the region and share it with people in defensive needs in these countries.

It's increasingly difficult to make it happen, but, cross collaboration throughout the industry, a good cause for good, I think is why we're pursuing it ultimately. Thank you.

**Jamie Tarabay:** Emily, obviously, some of this, for every action is the equal opposite reaction.

We've seen a lot of reaction from the US, Australia, in the Pacific Islands, for example, Caroline Kennedy's been to Guadalcanal a bunch of times now, and there's been an uptick in diplomacy. You've been across this analysis of China's military civil fusion strategy, and you have a lot of insight on all of these different areas, in terms of economic and technology, technological and geopolitical change, what are the different ways that.. That, it's always a question of how do you, I don't want to say counter it, but how do you provide an alternative that doesn't feel like it's wrapped up in some kind of geopolitical context, or is that even possible anymore?

**Emily de La Bruyère:** Yeah, that's a real doozy of a question.

I think to address it I want to start by building on a little bit of what Tom just said about, what the kind of risk that stems from these Chinese footholds, if you will, is and how Beijing can use them. And there was a point in there, A, there's, the espionage, the direct cyber attack risk.

There's also the leverage Beijing gets, like broader political leverage, social leverage, economic leverage from the reliance on it. and reliance that's not just countries need infrastructure, countries need telecommunications inputs, but also the awareness that Beijing could, if it so wished, attack these foundational critical infrastructures, stop them from working, distort them.

The degree to which that can then infringe, maybe in a subtler way on political autonomy, I think is really important to understand in terms of why China's digital strategy is a threat, and also what military civil fusion entails.

Another point just on this front is that when we talk about this in Beijing's presence in these footholds and potential for coercion or attack, this isn't just a question of Huawei and Huawei inputs.

I think that there's a tendency to simplify in that direction, because Huawei so is the poster child for what Beijing is doing and for military civil fusion and this kind of coercive technological strategy, but there are any number of other Huawei's out there and other Huawei's at different stages of the value chain or in other digital value chains.

That means that, which is finally going to get to your question, there can be moves like bans or restrictions on Huawei equipment, and there can be efforts to create alternatives to Huawei, but all of that is not only reactive and one step behind, but also only addressing a small percentage of what the actual problem is.

The reality that Beijing is shaping an environment, not just attacking like a tactical node or a tactical point. You can make the same argument in terms of the more proactive diplomacy that the U. S. has been conducting. By and large, when the U. S. and allies and partners, as you said, go out to other countries, work, try to provide an alternative, provide alternatives, we're doing so in a more reactive way, where China's already been there, or China's already had a foothold.

At the best, we're one step behind, and we're one step behind in a relatively small sliver of where Beijing's exerting influence. My sense is what that means is that this kind of an approach, the we're going to fight the tactical battles approach, so we're going to focus on a supply chain or a country, that's never going to work.

China's always going to be there first, both because of the nature of the Chinese system, and because of the whole, hider finder or, shaping the initiative nature of competition. That demands an approach that is more about the strategic layout, more about the environment, more about making sure that the international system is continuing to defend itself as an international system, so there isn't room for a bad actor to go out there and be proliferating technical systems that have backdoors built in, or to be distorting markets in a way that then creates massive dependencies on it and coercive leverage on it.

That's a matter fundamentally of the international system, whether that's standard setting bodies that have stronger requirements for safety, and for norms, or that's organizations like the World Trade Organization stepping up and saying here are our actual free trade rules for the international system and here's how we're going to enforce them. Until the U. S., its allies and partners, are out there actually making sure that we're strengthening a rules based world order, China is going to be shaping this competition and effectively deciding who wins.

**Jamie Tarabay:** We have to go to questions, but before we do, Mallory, do you want to, I feel like there's something for you to add here on this.

**Mallory Knodel:** No, I mean, I just really appreciate all the expertise on this panel. It's also given me a lot to think about as I continue to engage in this. I think that's a really important piece of this highly technocratic space because I want to maybe that's

something to highlight is, the more we allow some of these riffs, some of these political questions to play out in technical standards bodies, the more we're actually playing on China's strengths and on its own territory.

So, I want to caution that we don't imagine that these are just technocratic battles, that in fact, they are highly political. Right now I, at least from my purview, again, on the technology side, but at CDT, we also do a lot of policy. I've done global internet governance for a long time. It seems to me that the real political battles and the stages for those battles are weakening. This maybe speaks to Emily's point about rules based order.

And so, we're shoving these deeply political issues into a technocratic space, and that can only benefit sort of technocratic regimes and autocratic tendencies, so I just want to say that's something that we need to factor into our calculus on how some of this gets resolved, where we meet, some of these battles and what we take on and where. That sort of real question of mandate and best placed stages to have these battles is really important.

Thanks.

**Jamie Tarabay:** I think there's also this conversation about aid versus loans, right? And like, Tom, you also talked about sort of the financial side of it as well, and how fraught that can be, that it becomes this inescapable, injurious loan versus, aid, and what are the guidelines, or the sort of the guideposts, to sort of navigate that in a way that doesn't feel like it is just as, sort of, penalty driven?

**Tom Hegel:** Yeah, It's a challenge, at no fault of their own throughout Africa, we see organizations, that are in the position where they have no other option for pursuing a thriving country, Chinese investments is probably the only option, because the lack of Western investments in the region is undeniable in many cases. That's why we see organizations, like the African Union, that are more interested in pursuing Chinese technology and okay with that risk because of the lack of Western investments.

Giving technology dominance to China isn't their concern. Their concern in many cases, again, no fault of their own, is to be able to get funding to be able to build roads, schools, critical infrastructure, so it's like a future problem. Right now, we just need to be able to function as a nation. So it's, in many cases, not like a bit of an afterthought, but just less of a priority.

It's tricky because you're also facing a scenario where the only nations in Africa that are pushing against Chinese investment are landlocked and surrounded by neighbors that are all dominated by Chinese technology, financial communications and so forth, so, in many cases, they're losing out when they're not doing that as well.

There's not an easy answer to it, unfortunately, but Western investment definitely needs to step up to be able to challenge this at all, in my opinion.

**Jamie Tarabay:** Right. So, there's a question. I'm going to throw it to all of you. We certainly see the allure for authoritarian countries in this vision of the Internet, has any of you seen any global South countries, however, that are actively pushing back on this vision, specifically addressing the political implication of this system? In terms of the global South, are you seeing any, like, real examples of pushback? I think what you just said, Tom, about landlocked African countries that are surrounded by neighbours that... are there any other examples in South America, perhaps, in South Asia, that we're seeing a similar process happening?

**Tom Hegel:** Yeah. It's a good question. I'll avoid naming any countries right now just because I don't want to be inaccurate. But, from a high level perspective, there are certainly countries that are pushing back. By and large, we're seeing direct specific types of investments, or specific types of projects, being pushed back on, for the most part, investments coming from certain banking organizations in China, that might not be apparently state sponsored, things like that, are a little easier to get into your organization, a little easier to bypass that global perspective of China's investing in your country and taking it over.

It's that traditional soft power agenda from China, long term plays that are happening. So, even if, you are one of those organizations or those countries that's pushing back, you are eventually going to have some sort of overlap in Chinese investments, or something from China, if that's what you're surrounded by constantly, especially with the lack of investment otherwise.

So, yeah, Africa is an easy example, but, Latin America is... this type of stuff is dominating out there as well. I would say. Latin America, in many cases, is a bit younger in the play, the long term agenda of China. We're not seeing it already completely dominated by Chinese telecommunications, for example, it's a newer thing. A lot of the geopolitical events unfolding throughout Latin America as well are changing up the landscape as well.

So yeah, it's a long story to answer. No, I don't know. I'll avoid naming countries right now, but, yeah, there's certainly some, but things are changing quickly.

It's hard to say for certainty.

**Jamie Tarabay:** It's definitely a place to watch. Dakota, did you want to jump in?

**Dakota Cary:** Yeah. The country that sticks out in Latin America for me is Costa Rica, as trying to like effectively balance between the U S and PRC systems. Costa Rica is taking

on a good bit of investment from PRC, and has spurned putting Chinese made tech into their infrastructure.

In fact, they recently signed a cybersecurity agreement with the United States. That cybersecurity agreement included a bunch of aid to help Costa Rica recover from a pretty significant ransomware event, from a Russia linked actor. And so, we see this convergence and competition between larger nations within Costa Rica, where China is trying to win favor.

It is promoting its usual wares through infrastructure investments, et cetera, but also trying to get into the internet and telecommunications infrastructure stack. I wouldn't say that there are causal links between any of the events, but I do think that the U. S. stepping in and having a cybersecurity agreement along with funding and aid to improve cybersecurity in Costa Rica is a really good example, that the competition is ongoing.

There are no foregone conclusions, nobody has won, and that countries still are making incredibly difficult decisions about trying to get what their people need, which is both infrastructure that is roads, and infrastructure that is digital highways.

**Jamie Tarabay:** Go ahead, Emily.

**Emily de La Bruyère:** If I could just jump in there, the Costa Rica point, I think, suggests something, and I'm not by any means an expert in the Global South, but my sense, speaking to international audiences, and observing what's going on has been that the largest draw, or the largest reason, to push back at Chinese systems, for better or for worse, has not been the political implication, it's been the draw of US and European especially markets, and political ties that are seen as contradictory with falling into the Chinese technological sphere of influence. There's definitely a much more market based version, or element, to what the logic is, which I think is very important to keep in mind from the US perspective in terms of messaging, and what tools are going to be most effective.

**Jamie Tarabay:** So, there is a path, Mallory?

**Mallory Knodel:** Yeah, I certainly think so. I would add one data point to what others have said, which is also these diplomatic networks that the U. S. is invested in, like the Freedom Online Coalition, that they're really focused on getting more members of that from the Global South, and that I think offers something a little softer, but that I think is part of the importance for some of these Global South countries, because they don't just want to have these roads, or these networks, it is also about building coalition and alliance, and that is where we started with the Open Internet, circa 2011, Hillary Clinton, Secretary of State, Internet Freedom proposition, that's actually been pretty effective. It's starting to erode, but this sort of approach harkens back to that, and it can be compelling for global South states where it is more participatory.

The declaration for the future of the Internet, and things like that, that are also trying to meet those sort of ideals around openness, from civil society and activists, those still give me chills. Those are still the things that are compelling.

I'm glad to know that states really want that too. It goes beyond just the protocols, and the markets, and things like that. All of these layers are really important.

**Jamie Tarabay:** It just occurred to me that we've spent the better part of an hour talking about tech and we didn't once mention AI, which is a miracle because I feel like that's a whole other conversation we could be having right now.

I just wanted to say thank you. We are out of time, but I want to appreciate the comments and really smart analysis and insight from Mallory, Tom, Emily and Dakota. Hopefully the Atlantic Council has Dakota's report online, and I appreciate all your questions. I'm sorry we didn't get to them all and, hopefully, we can all get together and chat about this and more in the future.

**Dakota Cary:** Thank you so much

**Emily de La Bruyère:** Can I say just kudos to Dakota on a really fantastic report, that fills also a much needed gap.